UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of	) 4:22 MJ 8042 SRW
INFORMATION ASSOCIATED WITH KiK USERNAMES painandcuddle_5im, painandcuddle, pain7x6_66v, pain7x6, open7x6_p3o, open7x6, temp7x6 and temp7x6_4ch THAT ARE STORED AT PREMISES CONTROLLED BY KIK c/o MEDIALAB, INC.	) **FILED UNDER SEAL**) SIGNED AND SUBMITTED TO THE COURT FOR) FILING BY RELIABLE ELECTRONIC MEANS)

APPLICATION FOR A SEARCH WARRANT

I, Jacob Walk, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A

located in the _____ District of California, there is now concealed

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

xx evidence of a crime;
xx contraband, fruits of crime, or other items illegally possessed;
xx property designed for use, intended for use, or used in committing a crime;
a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title Section	

Title 18, United States Code, Sections 2251(a) (sexual exploitation of children), 2252A (certain activities relating to material constituting or containing child pornography), 2422 (coercion and enticement of a minor) and/or 1470 (transfer of obscene material to a minor)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

✓ Continued on the attached sheet.
❑ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the following is true and correct.

_____
Applicant's signature
Jacob Walk, SFO, FBI
Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date 01/21/2022

_____
Judge's signature

City and State: St. Louis, MO

Honorable Stephen R. Welby, U.S. Magistrate Judge
Printed name and title

AUSA: Jillian Anderson

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH KiK USERNAMES painandcuddle_5im, painandcuddle, pain7x6_66v, pain7x6, open7x6_p3o, open7x6, temp7x6 and temp7x6_4ch THAT ARE STORED AT PREMISES CONTROLLED BY KIK c/o MEDIALAB, INC.	))))))	No. 4:22 MJ 8042 SRW **FILED UNDER SEAL** **SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jacob Walk, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Criminal Procedure 41 for information associated with painandcuddle_5im, painandcuddle, pain7x6_66v, pain7x6, open7x6_p3o, open7x6, temp7x6 and temp7x6_4ch (the "subject accounts") that are stored at premises owned, maintained, controlled, or operated by Kik c/o Medialab, Inc., (formerly "KiK Interactive, Inc.") a social-networking company headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. The requested warrant would require Kik c/o Medialab, Inc. to disclose to the United States records and other information in its possession, including the contents of communications, pertaining to the subscriber or customer associated with the subject account as further described in Attachment B.

2. I am a Special Federal Officer (SFO) with the Federal Bureau of Investigation's ("FBI") Child Exploitation Task Force. I have been a Special Federal Officer for eight years and have been a sworn Deputy with the Franklin County Sheriff's Office for seventeen years. I have conducted numerous investigations regarding the sexual exploitation of children that involve the use of a computer which has been used to commit a crime in violation of Title 18, United States Code, Sections 2251 and 2252 (sexual exploitation of a child), Title 18, United States Code, Section 2252A (child pornography) and Title 18, United States Code, Section 2421 (transportation with intent to engage in criminal sexual activity). As a Task Force Officer, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been personally involved in the execution of search warrants to search residences and seize material relating to the sexual exploitation of minors including computers, computer equipment, software, and electronically stored information. I have experience utilizing computers during my career as an investigator and I have completed multiple in-service training, outside training, and other courses in computer crime investigation.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1470, 2251, 2252, 2252A and 2422 have been committed by Mark Tucker and other unknown persons and which criminalize, among other things, transferring obscene materials to minors, the

possession and/or receipt and shipment of child pornography, and enticement of minors to engage in any sexual activity for which a person can be charged with a criminal offense. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED

5. The location to be searched are the accounts and accounts associated with usernames:

painandcuddle_5im
painandcuddle
pain7x6_66v
pain7x6
open7x6_p3o
open7x6
temp7x6_4ch
temp7x6

that are stored at premises owned, maintained, controlled, or operated by Kik c/o Medialab, Inc., located at 1237 7th Street, Santa Monica, California 90401, further described in Attachment A. The items to be reviewed and seized by the United States are described in Attachment Part II of Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO Kik

7. The Internet is in part a computer communications network using interstate and foreign telephone and communication lines to transmit data streams, including data streams used to provide a means of communication from one computer to another and used to store, transfer and receive data and image files.

8. An "Internet Protocol" (IP) address is a unique series of numbers, separated by a period, that identifies each computer using, or connected to, the Internet over a network. An IP address permits a computer (or other digital device) to communicate with other devices via the Internet. The IP addresses aids in identifying the location of digital devices that are connected to the Internet so that they can be differentiated from other devices. As a mailing address allows a sender to mail a letter, a remote computer uses an IP address to communicate with other computers.

9. An "Internet Service Provider" (ISP) is an entity that provides access to the Internet to its subscribers.

10. The term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

11. Kik is a smartphone messenger application that lets users connect with their friends and the world around them through chat. Users can send text, pictures, videos, and more-all within the application. Kik is available for download through the iOS App Store and the Google Play store on most iOS (iPhone/iPod/and iPad) and Android (including Kindle Fire) devices. Kik is free to download and uses an existing Wi-Fi connection or data plan to send and receive messages.

12. Unlike many other smartphone messaging services which are based on a user's phone number, Kik uses usernames as the unique identifier. By using the usernames instead of phone numbers, users' personal information is never shared by Kik. If a Kik user is an active user of other social apps and sites, they might choose to share their username on those sites to connect with their followers from there. If a user posts his/her Kik username somewhere like Twitter or Instagram, or on a Kik optimized webpage, will make it publicly available.

13. The "New Chats" feature gives users control over who they talk to. This safety feature puts messages from new people in a separate section called "New Chats." In messages from new people, picture, or content messages they may have sent are blurred, with the option to unblur and view the content. A user has the option to either start a chat with them, delete, block, or report.

14. A Kik username is unique, can never be replicated, can never be changed, and is the only publicly available identifier used to identify a Kik account. Kik cannot identifier users using phone numbers, first and last name (display name), or email address. The exact Kik username must be provided to conduct any search in the Kik system.

15. A "Group Hashtag" (Public Groups) is a user-generated hashtag, can never be replicated, can never be changed, and will begin with the hashtag symbol (#).

16. A Group Scan Code can be used for private and public groups. It can be accessed through the group profile information page and users can share the scan code to invite others to join.

17. JIDs are unique internal IDs associated to users and group chats, randomly generated by Kik's internal systems. JIDs are not public-facing. A user JID is a username followed by an underscore and three additional characters that are randomly assigned by Kik for

every username. A group JID is a 13-digit numeric string followed by "_g." It will not contain alphabetical characters (other than the "_g"), periods, spaces, or emoticons.

18. A content ID is a unique ID associated to a media file sent on Kik. The format of a Kik content ID is eight alphanumeric characters, dash, four alphanumeric characters, dash, four alphanumeric characters, dash, four alphanumeric characters, dash, twelve alphanumeric characters.

19. As explained herein, information stored in connection with a Kik account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Kik user's account activity, IP log, stored electronic communications, and other data retained by Kik, can indicate who has used or controlled the Kik account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Kik account at a relevant time. Further, Kik account activity can show how and when the account was accessed or used. For example, as described herein, Kik logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Kik access, use, and events relating to the crime under investigation. Additionally, Kik builds geo-location into some

of its services. Geo-location allows, for example, users to "tag" their location in posts and Kik "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Kik account owner. Last, Kik account activity may provide relevant insight into the Kik account owner's state of mind as it relates to the offense under investigation. For example, information on the Kik account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

20. Based on the information above, the computers of Kik c/o Medialab, Inc. are likely to contain all the material described above with respect to the SUBJECT ACCOUNT, including stored electronic communications and information concerning subscribers and their use of Kik, such as account access information, which would include information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

PROBABLE CAUSE

DEFINITIONS

21. The following terms have the indicated meaning in this affidavit:

a. The term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device. 18 USC § 1030(e).

b. The term "minor" means any individual under the age of 18 years. 18 USC § 2256(1).

c. "Sexually explicit conduct" means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or

masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person. 18 USC § 2256(2).

d. "Visual depiction" includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. 18 USC § 2256(5).

e. "Child pornography" means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 18 USC 2256 § (8)(A) and (C).

f. "Identifiable minor" means a person who was a minor at the time the visual depiction was created, adapted, or modified; or whose image as a minor was used in creating, adapting, or modifying the visual depiction; and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and shall not be construed to require proof of the actual identity of the identifiable minor. 18 USC § 2256(9).

g. The Internet is a computer communications network using interstate and foreign telephone lines to transmit data streams, including data streams used to provide a means of communication from one computer to another and used to store, transfer and receive graphic image files.

INVESTIGATION

22. On April 23, 2021, your affiant was assigned a cyber tip from the National Center for Missing and Exploited Children. According to the cyber tip, an electronic service provider (ESP) reported a user with the username "painandcuddle" and user ID of "painandcuddle_5im", created February 26, 2021, uploaded twenty-eight (28) video files of apparent child pornography which were viewed by the ESP, according to the cyber tip.

23. The Kik user account painandcuddle was created February 26, 2021 according to records provided by Kik along with the cyber tip. The records also indicated the first and last name of the account is "Jim Bob."

24. Your affiant viewed the nineteen reported video files, some of which are duplicates, and confirmed some of the videos depict minor pre-pubescent children involved in sexual acts while others are considered age difficult, meaning your affiant is unable to determine if the individual in the video is a minor or adult.

25. The ESP reported the video files were uploaded from IP addresses 24.217.233.152, 71.11.150.38, 166.170.233.3 and 166.175.62.252. The cyber tip reported IP addresses 24.217.233.152 and 71.11.150.38 are assigned to Charter Spectrum and IP addresses 166.170.233.3 and 166.175.62.252 are assigned to AT&T Wireless, which your affiant knows from prior investigations does not maintain account holder information for customers utilizing their IP addresses.

26. The following are some of the files uploaded from the IP address of 24.217.233.152, between March 15th and March 19th 2021, are described below:

a. File name**:** dae22d5f-55ab-466b-abee-3cae92c922d3.mp4
MD5 - 656a631bd79ce8d6b86326bbf28e0982

Description: A video file, 59 seconds in length, depicting an age difficult male performing oral sex on a nude prepubescent minor female in a bathtub. The female is determined prepubescent due to the lack of body hair, overall small stature and lack of anatomical growth.

b. File name: 6f5729f9-7bfe-4296-a543-08c4a897a673.mp4
MD5 - 853f1a161cdcdecfa80294f96ca0d534

Description: A video file, 1 minute 45 seconds in length, depicting a prepubescent minor male attempting to engage in vaginal intercourse with a prepubescent minor female at the direction of another individual off camera. The minors are determined prepubescent due to the lack of body hair, overall small stature and lack of anatomical growth.

c. File name: 4361fb66-1230-44f1-b360-b09f7fcffc66.mp4
MD5 - 9fc37628f1c4519a117a2a616e085107

Description: A video file, 1 minute 59 seconds, in length depicting an age difficult female performing oral sex on a prepubescent minor male. The male is determined prepubescent due to the lack of body hair, overall small stature and lack of anatomical growth.

d. File name: e27d317f-45b2-4b2c-ab9b-74f8270d218b.mp4
MD5 - 00924aeacce094bf8c6b300674607229

Description: A video file, 40 seconds in length, depicting a prepubescent minor male engaged in vaginal intercourse with a prepubescent minor female while being held by an adult female. The hand of another individual, who is off camera, can be seen rubbing the breast of the adult female. The minors are determined prepubescent due to the lack of body hair, overall small stature and lack of anatomical growth.

e. File name: bd6a241f-1e2e-42fb-87be-a12615e446f8.mp4Sha1
MD5 - 0e22fdf3289f886e463dbc7329b8470c

Description: A video file, 40 seconds in length, depicting an adult female performing orals sex on a prepubescent minor male. The male is determined prepubescent due to the lack of body hair, overall small stature and lack of anatomical growth.

f. File name: 99ca3226-d657-4b9f-887c-85646302b8a5.mp4
MD5 - 2a6b8cc1b30d3f95ab509bdd016e4578

Description: A video file, 1 minute 58 seconds in length, depicting an age difficult female performing orals sex on a prepubescent minor male. Later in the video the age difficult female directs the prepubescent minor male to engage in vaginal intercourse with her. The male is determined prepubescent due to the lack of body hair, overall small stature and lack of anatomical growth.

g. File name: 14047517-7183-4a79-b28d-2cc2046a5d5a.mp4
MD5 - 1b8be3085d03a0a3f99eefc3fd447faa

Description: A video file, 1 minute 10 seconds in length, depicting an age difficult female performing orals sex on a prepubescent minor male. The male is determined prepubescent due to the lack of body hair, overall small stature and lack of anatomical growth.

h. File name: 47c36d0c-5016-4412-9fa0-72e94c9095e2.mp4
MD5 - 90657cd43ab7ddc27be248484fa36a42

Description: A video file, 15 seconds in length, depicting a prepubescent minor female engaged in vaginal intercourse with a prepubescent minor male. The video

is recorded by a third party off camera that assist putting the minor male's penis into the vagina of the minor female. The minors are determined prepubescent due to the lack of body hair, overall small stature and lack of anatomical growth.

i. File name: e1dedd2f-002c-4b4b-aab8-5c50db245dfd.mp4
MD5 - 118dd2df0f36bbf318937c4888cf7fe2

Description: A video file, 14 seconds in length, depicting a prepubescent minor female performing oral sex on an adult male. The minor female is determined prepubescent due to the lack of body hair, overall small stature and lack of anatomical growth.

27. The following is one of the files uploaded from the IP address of 71.11.150.38, on March 17th, 2021, are described below:

a. File name: 8dc79e4f-5141-4529-a384-46e335472fc6.mp4
MD5 - 1ac55257e11077991c0a75b58cbf98d1

Description: A video file, 1 minute 28 seconds in length, depicting two minor prepubescent female's nude in a bathtub with an adult male. One of the minor females performs orals sex on the adult male prior to the adult male rubbing his penis between the legs of the other prepubescent female near her vagina. The females are determined prepubescent due to the lack of body hair, overall small stature and lack of anatomical growth.

28. Affiant knows from training and experience that Internet computers identify each other by an Internet Protocol or IP address. Affiant knows that these IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead a law enforcement officer to a particular Internet service company and that company can typically identify the account that uses or used the address to access the Internet.

29. A Missouri State investigative subpoena was sent to Charter Spectrum by your affiant to identify the account holder information for IP addresses 24.217.233.152 and 71.11.150.38.

30. On August 31, 2021, your affiant received records from Charter Spectrum. According to Charter Spectrum, during the time of the uploads, IP address 24.217.233.152 was

assigned to account holder, Mark Tucker, with a service address as 803 Madison Avenue Washington, Missouri 63090. The billing address is shown to be 803 Madison Avenue Washington, Missouri 63090. Charter Spectrum identified the account holder of IP address 71.11.150.38 as City of St. Louis-Fire Repair Acad with a service and billing address of 1125 Spruce Street, CBN, St. Louis, Missouri 63102. Charter Spectrum also provided email addresses for the account holder which had email addresses beginning with "stlfd2446".

31. A check with the Franklin County Assessor's Office revealed 803 Madison Avenue Washington, Missouri is owned by Mark Tucker and J.M.T.

32. Your affiant contacted an FBI Task Force Officer employed by the St. Louis Metropolitan Police Department whom confirmed Mark Tucker is an employee of the St. Louis Fire Department.

33. On September 7, 2021, your affiant drove by 803 Madison Avenue Washington, Missouri 63090 and checked for any open wireless internet connections in the area from the street and determined there were no unsecured wireless connections directly in front of the residence. Also parked in the driveway of the residence were two motor vehicles registered to Mark Tucker and J.M.T. according to the Missouri Department of Revenue.

34. On September 3, 2021, your affiant was assigned cyber tip 9754833 and 97587081 from the National Center of Missing and Exploited Children (NCMEC). According to cyber tip 9754833, MediaLab/Kik reported a user uploaded thirty-one child pornography files. Kik identified the reported user with the following information:

a. Email Address: nehon4542@iludir.com
b. Username: pain7x6
c. User ID: pain7x6_66v

35. The Kik user account pain7x6 was created April 24, 2021 according to records provided by Kik along with the cyber tip. The records also indicated the first and last name of the account is “Jim Bob.”

36. I viewed the 31 reported uploaded video files and confirmed some of them depicted child pornography as other files are considered age difficult. The IP address the files were uploaded form were 155.186.32.222, 166.175.185.178, 166.175.185.192 and 166.170.223.160. According to the cyber tip, IP addresses 155.186.32.222 is assigned to Charter Communications, so a subpoena will be sought for account holder information for the customer assigned those IP addresses during time of the uploads. IP addresses 166.175.185.178, 166.175.185.192 and 166.170.223.160 are assigned to AT&T Wireless, whom I know from previous experience does not maintain account holder information for customers utilizing their IP addresses.

37. Included with the cyber tip from Kik was a subscriber data for the Kik account of pain7x6. According to the subscriber data, the first and last name on the account was "Jim Bob" and the type of device and model accessing the account was an iPhone.

38. According to cyber tip 97587081, MediaLab/Kik reported a user uploaded twenty-six child pornography files. Kik identified the reported user with the following information:

a. Email Address: meseyo7000@nnacell.com
b. Username: open7x6
c. User ID: open7x6_p3o

39. The Kik user account open7x6 was created July 3, 2021 according to records provided by Kik along with the cyber tip. The records also indicated the first and last name of the account is “Jim Bob.”

40. I viewed the 26 reported uploaded video files and confirmed some of them depicted child pornography as other files are considered age difficult. The IP address the files were uploaded form were 155.186.32.222, 166.175.187.213, 166.175.187.202 and 166.170.222.124. According to the cyber tip, IP addresses 155.186.32.222 is assigned to Charter Communications, so a subpoena was later sought for account holder information for the customer assigned those IP addresses during time of the uploads. IP addresses 166.175.187.213, 166.175.187.202 and 166.170.222.124 are assigned to AT&T Wireless, whom I know from previous experience does not maintain account holder information for customers utilizing their IP addresses.

41. Included with the cyber tip from Kik was a subscriber data for the Kik account of open7x6. According to the subscriber data, the first and last name on the account was "Jim Bob" and the type of device and model accessing the account was an iPhone.

42. On September 16, 2021, a federal search warrant was executed at 803 Madison Avenue Washington, Missouri 63090. Mark Tucker was located living in the residence.

43. During questioning, Mark Tucker admitted to using the application Kik. ." I asked Mark Tucker if he ever had a username on Kik of painandcuddle and he responded, "I did, I don't remember so."

44. Your affiant asked Mark Tucker what first and last name does he use on his Kik accounts and he replied, "I have no idea." I asked if he used the name "Jim Bob" and he replied, "I have no idea" and "it’s been awhile." Mark Tucker refused to answer any further questions shortly thereafter.

45. On September 27, 2021, I received records from Charter Communications pursuant to a federal subpoena for account holder information for 155.186.32.222, target date

range from 6/19/2021 at 12:08:21 UTC to 8/7/2021 at 00:11:20 UTC. According to the records, the IP address was assigned to:

a. Mark Tucker a
b. 803 Madison Avenue
c. Washington, Missouri 63090

46. 803 Madison Avenue, Missouri 63090 is the same residence the search warrant was executed at on September 16, 2021.

47. On December 30, 2021, your affiant was assigned another cyber tip, 102759139, MediaLab/Kik reported a user uploaded four child pornography files On August 30, 2021. Kik identified the reported user with the following information:

a. Email Address: xudafa@thichanthit.com
b. Username: temp7x6
c. User ID: tempt7x6_4ch

48. The Kik user account temp7x6 was created August 30, 2021 according to records provided by Kik along with the cyber tip. The records also indicated the first and last name of the account is "Jim Bob." According to the cyber tip, all of the child pornography files were uploaded from IP address 155.186.32.222, which Charter Communications already confirmed is assigned to Mark Tucker at 803 Madison Avenue Washington, MO 63090.

49. Based on the above information, there is probable cause to believe that the items listed in Attachment A constitute evidence of violations of Title 18, United States Code, Sections 2251, 2252 and 2252A and will be found in the electronic or wire communications stored by **Kik c/o MediaLab.ai Inc.** located at 1237 7th Street Santa Monica, CA 90401.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

50. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), (b)(1)(A), and (c)(1)(A), by

using the warrant to require Kik c/o Medialab, Inc. to disclose to the United States copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, United States-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

51. Based on the forgoing, I request that the Court issue the proposed search warrant.. The United States will execute this warrant by serving the warrant on Kik. Because the warrant will be served on Kik, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

52. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

53. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution,

using the warrant to require Kik c/o Medialab, Inc. to disclose to the United States copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, United States-authorized persons will review that information to locate the items described in Section II of Attachment B.

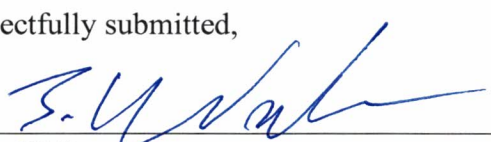
CONCLUSION

51. Based on the forgoing, I request that the Court issue the proposed search warrant.. The United States will execute this warrant by serving the warrant on Kik. Because the warrant will be served on Kik, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

52. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

53. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Jacob Walk
Special Federal Officer

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Kik profile, Kik accounts and Kik accounts associated with usernames:

painandcuddle_5im

painandcuddle

pain7x6_66v

pain7x6

open7x6_p3o

open7x6

temp7x6_4ch

temp7x6

that are stored at premises owned, maintained, controlled, or operated by Kik c/o Medialab, Inc., located at 1237 7th Street, Santa Monica, California 90401.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Kik c/o Medialab, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Kik c/o Medialab, Inc., including all content, messages, records, files, logs, transactional data or information that have been deleted but are still available to Kik c/o Medialab, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Kik c/o Medialab, Inc. is required to disclose the following information from February 26, 2021 to the date this warrant is received to the United States for each account listed in Attachment A:

Non-Content User Data

(a)Basic Subscriber data;

(b) Current first and last name and email address;

(c)Link to the most current profile picture or background photo;

(d) Device related information;

(e)Account creation date and Kik version;

(f) Birthdate and email address used to register the account;

(g) User location information, including IP address(es).

Content Data

(a)IP addresses associated to the accounts;

(b) All transactional chat logs associated to the accounts;

(c) All images and video associated to the accounts including the unknown usernames; and IP address associated to the sender of the images and video;

(d) A date-stamped log showing the usernames that accounts added

and/or blocked;

(e) All abuse reports associated to the Kik accounts including the unknown usernames;

(f) All emails associated to the accounts;

(g) Registration IP address associated to the accounts;

(h) All user content created, uploaded, or shared by the accounts, including any comments made by the accounts on photographs or other content;

(i) All location data associated with the accounts created, uploaded, or shared by the accounts;

(j) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(k) All past and current usernames associated with the accounts;

(l) All records of Kik searches performed by the accounts, including all past searches saved by the accounts;

(m) All activity logs for the accounts and all other documents showing the user's posts and other Kik c/o Medialab, Inc. activities;

(n) All photos and videos uploaded by that accounts and user ID and all photos and videos uploaded by any user, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(o) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that accounts and user ID, including the hardware

model, operating system version, unique device identifiers, mobile network information, and user agent string;

(p) All IP logs, including all records of the IP addresses that logged into the accounts;

(q) The types of service utilized by the user;

(r) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(s) All privacy settings and other account settings, including privacy settings for individual posts and activities, and all records showing which Kik users have been blocked by the accounts;

(t) A list of all of the people that the user follows on Kik and all people who are following the user (*i.e.*, the user's "following" list and "followers" list), as well as any friends of the user;

(u) A list of all users that the accounts have "unfollowed" or blocked;

(v) All privacy and account settings;

(w) All information about connections between the accounts and third-party websites and applications; and,

(x) All records pertaining to communications between Kik c/o Medialab, Inc. and any person regarding the user or the user's Kik accounts, including contacts with support services, and all records of actions taken, including suspensions of the accounts.

(y) Any and all cookies associated with or used by any computer or web browser associated with the accounts, including the IP addresses, dates, and times associated with the recognition of any such cookie;

(z) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(aa) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Kik c/o MediaLab.ai Inc. user identification numbers; groups and networks of which the user is a member, including the groups' Kik c/o MediaLab.ai Inc. group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Kik c/o MediaLab.ai Inc. applications;

(bb) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(cc) All "check ins" and other location information;

(dd) All records of the account's usage of the "Like" feature, including all Kik c/o MediaLab.ai Inc. posts and all non- Kik c/o MediaLab.ai Inc. webpages and content that the user has "liked"; and

(ee) All information about the Kik c/o MediaLab.ai Inc. pages that the account is or was a "fan" of.

Kik c/o Medialab, Inc. is hereby ordered to disclose the above information to the United States within 14 days of the date of this warrant.

II. Information to be seized by the United States

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1470, 2251, 2252, 2252A or 2422 involving [Mark Tucker and other unknown persons including, for each account or user ID identified on Attachment A, information pertaining to the following matters:

(a) Any correspondence pertaining to the persuasion, inducement, and/or enticement of a minor to engage in any sexual act or sexual contact, including all opened or unopened messages;

(b) Any messages, opened or unopened, where the message or the content of the message indicates contact with individuals regarding the sexual exploitation of children including the production, transportation, receipt or possession of visual depictions of minors engaged in sexually explicit conduct;

(c) Correspondence between these accounts and any other Facebook account where the content of the message discusses the sexual exploitation of a child including the production, transportation, receipt or possession of visual depictions of minors engaged in sexually explicit conduct, including all opened and unopened messages;

(d) Any message, opened or unopened, and any image or video file involving the sexual exploitation of a child including the production, transportation, receipt or possession of visual depictions of minors engaged in sexually explicit conduct which is attached to the message;

(e) Any file containing visual depictions of minors engaged in sexually explicit conduct;

(f) Any message, opened or unopened, and any image file that appears to contain passwords or information regarding encryption;

(g) Any information or records reflecting associates, accomplices or conspirators;

(h) Any evidence that indicates the account holders' state of mind as it relates to the crimes under investigation.

(i) All records and communications involving Mark Tucker.

(j) All records and communications concerning transferring obscene materials to minors, the possession and/or receipt and distribution of child pornography, and enticement and grooming of minors for the purpose of engaging in any sexual activity for which a person can be charged with a criminal offense.

(k) Evidence indicating how and when user's accounts were accessed to determine the chronological context of account use, account access, and events relating to the crime under investigation;

(l) Evidence indicating the account users' state of mind as it relates to the crimes under investigation;

(m) The identity of the person(s) who created the accounts, including records that help reveal the whereabouts of such person(s).

(n) The identity of the person(s) who created or used the user IDs, including records that help reveal the whereabouts of such person(s).

(o) Evidence indicating how and when the Kik accounts were accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crimes under investigation and to the Kik account owner(s);

(p) Evidence indicating the Kik account owners' state of mind as it relates to the crimes under investigation;

(q) The identity of the person(s) who created or used the user IDs, including records that help reveal the whereabouts of such person(s).